System, Method and Structure for Generating and

Using A Compressed Digital Certificate

(A-70555/RMA)

WE CLAIM:

1. A computer program product for use in conjunction with a computer system having a server and a client, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism, comprising: a program module that directs the computer system and/or components thereof including at least one or the client or server, to function in a specified manner to provide message communications, the message communications occurring in a computer system hardware architecture neutral and operating system neutral and network transport protocol neutral manner for representing a digital certificate, the program module including instructions for:

A. using a common data object header in substantially all communicated data including communicated certificates;

B. providing a plurality of public keys including a first public key and a second public key in a single certificate, each of said at least first and second public keys being associated with its own purpose;

C. providing a Tag Field that functions as a discriminator of different Certificates issued to the same Subject; and

D. representing a Subject Name and a Certificate Issuer Name in one fixed character set determined by the Version Field.

2. A hardware architecture neutral and operating system neutral and network transport neutral method for representing a digital certificate that enables at least encryption and digital signatures using substantially less storage and bandwidth than conventional digital certificates, said method comprising:

A. using a common data object header in substantially all communicated data including communicated certificates;

B. providing a plurality of public keys including a first public key and a second public key in a single certificate, each of said at least first and second public keys being associated with its own purpose;

C. providing a Tag Field that functions as a discriminator of different Certificates issued to the same Subject; and

D. representing a Subject Name and a Certificate Issuer Name in one fixed character set determined by the Version Field.

3. The method in claim 2, wherein said common data object header includes a plurality of fields including a Type field, a Version field, and a Content-Length field.

4. The method in claim 2, wherein said purpose is selected from the group of purposes consisting of encrypting messages, encrypting session keys, signing messages, signing and encrypting data, and combinations thereof.

5. The method in claim 3, wherein a single byte is used to represent a type and a version for the Type Field the Version Field; and three bytes are used to represent Content-Length in the Content-Length Field.

6. The method in claim 3, wherein a first single byte is used to represent a type in the Type Field and a second single byte is used to represent a Version in the Version Field; and two bytes are used to represent Content-Length in the Content-Length Field.

7. The method in claim 3, wherein each said byte has a length selected from the set of byte lengths consisting of 8 bits, 10 bits, 12 bits, 16 bits, 24 bits, 32 bits, 64 bits, 96 bits, and 128 bits.

8. The method in claim 3, wherein the Type field is used to identify that the object is a Certificate.

9. The method in claim 3, wherein the version number is used to represent at least one of the following attributes: (i) Algorithm used by Certificate Issuer to sign the certificate, (ii) Algorithm to be used with the Subject's first public key, (iii) Algorithm to be used the Subject's second or subsequent public key, (iv) Length of each public key, (v) Length of Certificate Issuer's signature, (vi) parameters for the algorithm, (vii) an exponent to use with RSA public key (viii) Character Set of Subject Name, and (ix) Character Set of Issuer Name.

10. The method in claim 3, wherein the version number is used to represent a plurality of attributes selected from the set of attributes consisting of: (i) Algorithm used by Certificate Issuer to sign the certificate, (ii) Algorithm to be used with the Subject's first public key, (iii) Algorithm to be used the Subject's second or subsequent public key, (iv) Length of each public key, (v) Length of Certificate Issuer's signature, (vi) parameter(s) for an algorithm, (vii) an exponent to use with RSA public key, (viii) Character Set of Subject Name, and (ix) Character Set of Issuer Name.

11. The method in claim 3, wherein the Version number is used to represent at least four attributes selected from the set of attributes consisting of: (i) Algorithm used by Certificate Issuer to sign the certificate, (ii) Algorithm to be used with the Subject's first public key, (iii) Algorithm to be used the Subject's second or subsequent public key, (iv) Length of each public key, (v) Length of Certificate Issuer's signature, (vi) parameter(s) for an algorithm, (vii) an exponent to use with RSA public key, (viii) Character Set of Subject Name, and (ix) Character Set of Issuer Name.

12. The method in claim 2, wherein said plurality of public keys include at least two public keys that have the same size (same length) and system parameters.

13. The method in claim 2, wherein said system parameters include an RSA Exponent or Diffie-Helman Generator.

14. The method in claim 2, wherein the Tag Field is treated as an unsigned integer that is incremented with each Certificate issued to the Subject.

15. The method in claim 2, wherein said unsigned integer has a four byte value.

16. The method in claim 14, wherein said treatment as an unsigned integer providing a mechanism for identifying which of a plurality of certificates having the same Subject Name is more recent than another certificate having that Subject.

17. The method in claim 16, wherein this treatment and mechanism replaces the validity dates found with X.509 or X.509-type certificates.

18. The method in claim 2, wherein the Tag Field is treated as ASCII characters to represent the expiration date of the Certificate.

19. The method in claim 18, wherein the Tag Field is treated as four ASCII characters to represent the expiration date of the Certificate as a two digit month number and a two digit year number.

20. The method in claim 2, wherein the Subject Name and Certificate Issuer Name are represented as two-byte characters.

21. The method in claim 20, wherein the two-byte characters comprise two-byte Unicode characters.

22. The method in claim 2, wherein the Version Field is used to indicate any additional fields that are present in the certificate.

23. A hardware architecture neutral and operating system neutral and network transport neutral method for representing a digital certificate that enables at least encryption and digital signatures using substantially less storage and bandwidth than conventional digital certificates, said method comprising the steps of:

using a common data object header in substantially all communicated data including communicated certificates;

providing a plurality of public keys including a first public key and a second public key in a single certificate, each of said at least first and second public keys being associated with its own purpose;

providing a Tag Field that functions as a discriminator of different Certificates issued to the same Subject; and

representing a Subject Name and a Certificate Issuer Name in one fixed character set determined by the Version Field;

said common data object header includes a plurality of fields including a Type field, a Version field, and a Content-Length field;

said purpose is selected from the group of purposes consisting of encrypting messages, encrypting session keys, signing messages, signing and encrypting data, and combinations thereof;

at most two bytes are used to represent a type and a version for the Type Field the Version Field; and at most three bytes are used to represent Content-Length in the Content-Length Field;

the Type field is used to identify that the object is a Certificate;

the Version number is used to represent a plurality of attributes selected from the set of attributes consisting of: (i) Algorithm used by Certificate Issuer to sign the certificate, (ii) Algorithm to be used with the Subject's first public key, (iii) Algorithm to be used the Subject's second or subsequent public key, (iv) Length of each public key, (v) Length of Certificate Issuer's signature, (vi) exponent to use with RSA public key, (vii) Character Set of Subject Name, and (vii) Issuer Name;

said plurality of public keys include at least two public keys that have the same size and the same system parameters;

the Tag Field is treated as an unsigned integer that is incremented with each Certificate issued to the Subject;

said treatment as an unsigned integer providing a mechanism for identifying which of a plurality of certificates having the same Subject Name is more recent than another certificate having that Subject;

the Tag Field is treated as ASCII characters to represent the expiration date of the Certificate;

the two-byte characters comprise two-byte Unicode characters; and

the Version Field is used to indicate any additional fields that are present in the certificate.

24. A method for representing a digital certificate, said method comprising:

using a common data object header in all communicated data including communicated certificates;

providing a plurality of public keys including a first public key and a second public key in a single certificate;

providing a first field that functions as a discriminator of different certificates issued to the same subject; and

representing a subject name and a certificate issuer name in one fixed character set determined by a second field.